Attacks with CryptoChameleon phishing kit target LastPass users

Date: 23rd April 2024 | Severity: High

Summary

LastPass is warning of a malicious campaign targeting its users with the CryptoChameleon phishing kit that is associated with cryptocurrency theft.

CryptoChameleon is an advanced phishing kit that was spotted earlier this year, targeting Federal Communications Commission (FCC) employees using custom-crafted Okta single sign-on (SSO) pages.

The phishing kit primarily targets the mobile devices of the employees and users of cryptocurrency companies and password management or single sign-on (SSO) service providers. In April 2024, LastPass issued a warning about a CryptoChameleon phishing campaign that targeted its customers using unsolicited phone calls and text messages.

The CryptoChameleon operators a combination of email, SMS, and voice phishing to trick users into clicking spoofed links of known cryptocurrency platforms (for example, Binance and Coinbase), email clients (for example, Gmail and Outlook), and password management solutions (for example, LastPass), and SSO providers (for example, Okta).

Attack Vectors

- The attacker combines multiple social engineering techniques that involve contacting the potential victim (voice phishing) and pretending to be a LastPass employee trying to help with securing the account following unauthorized access.
- Several social engineering tactics have been leveraged in the campaign, with attackers initially using an 888 number to contact targets regarding unauthorized LastPass account access before making another call impersonating a LastPass employee, who would send a phishing email with a link redirecting to a fraudulent website seeking the targets' master passwords, according to LastPass, which urged its users to be vigilant of suspicious phone calls, SMS messages, and emails amid fears of persistent targeting even after the shutdown of the malicious site.
- Such a development follows a Lookout report detailing attacks with the phishing kit that targeted the Federal Communications Commission and cryptocurrency platforms Coinbase, Binance, Gemini, and Kraken through spoofed Okta, Microsoft Outlook, Gmail, iCloud, and Twitter websites, among others.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domain	• 128147-coinbase.com • fcc-okta.com • lastpass.com. • 427883-coinbase.com • websitesusingthisphishingkit.mostofthewebsitesuseasubdomainofofficial-server.com • welcome-coinbase.com • unlink-coinbase.com • www-help-gemini.com • yphswappingwouldbeswitchingcapitalisandlowercaselstomakeacmeinc.com • unblock-coinbase.com • tokens-coinbase.com • tickets-apple.com • ticaltoacmelnc.com supportportal-coinbase.com • threat-coinbase.com • signin-kraken.com • startrecovery-coinbase.com • suite-trezor.io • server694590423.tech • security-umusic.com • secure-shakepay.com • restore-coinbase.com • secure-nexo.com • return-coinbase.com • registrationofdomainsusingcompanyname-okta.com • secure-binance.us • protect-gmail.com • recoverme-coinbase.com • protect-coinbase.com • protect-kraken.com • recoveryportal-coinbase.com • original-backend.com • protect-apple.com • prompt-coinbase.com • official-server.com • newpassword-coinbase.com • lookidenticaltoacmelnc.com • messages-coinbase.com • 826298-coinbase.com • identification-coinbase.com • keys-coinbase.com • helpdesk-gemini.com • helpdesk-icloud.com
URL	• http://shorturl.at/glvT0

Recommendation

- Increase education and awareness.
- Enable two-factor authentication.
- Deploy advanced mobile security.
- Verify the sender’s identity.
- Inspect the URL carefully.
- Keep your software up to date.
- Report suspicious activity.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.bleepingcomputer.com/news/security/cybercriminals-pose-as-lastpass-staff-to-hack-password-vaults/
- https://www.scmagazine.com/brief/attacks-with-cryptochameleon-phishing-kit-target-lastpass-users
- https://www.lookout.com/threat-intelligence/article/cryptochameleon-fcc-phishing-kit